Week 1 Notes

February-01-12
9:35 AM

SaaS – software as a service (design)

PaaS – platform as a service (OS)

IaaS – infrastructure as a service (switches)

SUS – software update services (test software updates first, then release them to end users)

TS – terminal services

Many remote desktop (users) -> TS -> authentication server (itm315 domain) <- resources

Security

- Network security (routers, switches)
    - Physical
    - logical (NOS – network OS)
    - Policy GPO – group policy options
    - File system security

Enterprise Network (system)

- Domain (root, root of forest) (microsoft)
    - Sales
    - North America (child domain for Microsoft)
        - Canada (child domain for north america)
            - Sales
                - User (Joe)
        - US
    - Europe
        - Sales
            - West
            - East
                - User (Nancy)
        - Italy
        - Sweden

Trust of relationships

- Trust is the foundation of domain security

a) Transitive (2-way trust)

A trusts B and B trusts A, B trusts C and C trusts B

- Domain is a security boundary, is used to
    - Authenticate users
    - Control access
    - Share resources
- Domain defines 2 types of objects
    - Container objec ex. OU
        - a container object contains sub-containers or leaf object
    - Leaf object (non-container)
        - User, printer, computer

Week 2 Notes

February-01-12
10:10 AM

Week 2 Notes

Note: the first domain installed in a network, automatically takes the role of the root domain → root of forest.

- Domain (root of forest) – AD
    - Child 1 - AD
    - Child 2 - AD
- Active directory: each domain has a "database" of all objects (users, groups, printers, OUs, computers) identified by this unique security ID (SID)
- An SID is a globally unique ID (GUID) that identifies an object and its attributes.
- Global Catalog: the root domain has an additional "database" call global catalog (GC)
    - A GC has partial information about all objects with a enterprise system.
        - All SIDs
        - Universal group membership
        - Object names of attributes
        - A pointer to other features (local domain membership)
        - Contains Domain Trust Relationship info
        - Allows users to log into the Domain using UNP
- UNP (user naming principal) has the following generic format: username@fully qualified domain name (FQDN)
    - Ex. nancy@child1.domain.com
- Domain vs DNS
    - Domain must have an authorized DNS server
    - DNS maps IPs to Names or names to IPs (name resolution)

- Note: to find out about your DNS IP address
    - nslookup
- or to find out the name of a DNS given its IP
    - nslookup 183.11.12.95
- if a name server (DNS) is not available you can NOT excess domain
- DNS follows the same format (structure) of a domain
    - .
        - Com (top level domain)
            - Microsoft (primary domain)
                - N America (secondary domain)
        - Org
        - Edu
- DNS controls communication between sites
    - Definition: in Microsoft network a site is defined by its range of IP addresses
        - 141.117.100.X site 1 toronto
            - Domain
            - Replica
        - 182.11.19.X site 2 vancouver
            - Child
            - Replica

- DNS maps IPs and names
- DNS major records:
  - A Host (authorize computers)
  - SRV server
  - SOA (start of authority) authorized DNS
  - PTR pointer – pointer to IP
  - NS name server
  - MX mail extension (exchange server)
- DHCP server: is used to assign authorized IPs to clients and assign an IP through 4 distinct steps called: DORA
  - Client -> discovery -> DHCP
    - Discovery: a client discover a DHCP server using a broadcast
      - msg: my IP is: 0.0.0.0, who is: 255.255.255.255
  - DHCP->offer->Client
    - DHCP offers an IP from its pool of IPs
  - Client->request->DHCP
    - Client must request the offered IP
  - DHCP->acknowledge->Client
    - DHCP acknowledges requested IP
- Dynamic update: (involves three parties)
  - Client
    - Get IP from DHCP: 182.11.14.8
    - Update DNS my IP 182.11.14.8 my A record: WS92
  - DHCP
    - Update DNS WS92 get 192.11.14.8
  - DNS
- Dynamic update notes:
  - DHCP assign an IP to client for default 8 days
  - It is client responsibility to update its IP before the expiring date
  - If a client request for an IP update, but the DHCP server is not available, the client assigned itself an IP called APIPA (automatic private IP address)
  - An APIPA has an address of 169.254.x.x
  - You can manually update your IP:
    - IPconfig /release
    - IPconfig /renew
- Replication
  - Multimaster domain vs master/slave structure
    - Windows NT
      - Primary domain controllers R/W
        - Master
          - Create objects
          - If master crashes
      - Backup secondary domain controllers R
        - Slave
          - Get a copy of objects
          - You need to promote slave to be a master domain
    - Windows 2008 server
      - Multimaster domain
        - Main domain R/W
          - replication
        - Replica domain R/W

- A user can log into any machine
- The info will be exchanged according to replication time set up
- Advantages: fault tolerant and load balancing

- Note: Win2k8 master domain support clustering feature
  - 141.117.11.1
    - Microsoft.com
  - 141.117.11.2
    - Microsoft.com
  - 141.117.11.3
    - Microsoft.com
  - 141.117.11.4
    - Microsoft.com
- Clustering allows us to have multiple domains using different IPs but the same DNS name.
  - Advantages: multiple replicas, load balancing, support many users
  - Disadvantages: bandwidth required and very expensive
- Replication time
  - Within a site
    - Domain<-link->replica
      - 3 seconds for normal replication (exchange user data)
      - For urgent replication (account lockout, account disabled)
        - Security related
        - No delay
  - Between 2 external sites
    - Domain(141.117.11.x)<-site link->replica(182.18.18x)
      - 90 minutes default
      - Security related, no delay

- Types of servers
  - Web server
    - 2 CPUs, IIS
  - Win2k8 standard edition
    - Used to upgrade from win2k3
      - 4 CPUs
  - Win2k8 enterprise edition
    - 8 CPUs
    - 8 clusters
  - Win2k8 datacenter (larger DBs)
    - 64 bit CPUs
    - Upto 32 CPUs
  - Hyper-V
    - Upto 32 CPUs
    - Supports upto 8 clusters
    - The foundation of MS cloud computing
    - Server virtualization
- Note: all versions support multitasking, multithreading operations through support of multiple processors called SMP
- SMP: symmetric multi-processors (load balanced CPUs)

Week 3 Notes

February-01-12
10:11 AM

Week 3 Notes

- Replication data is located in a folder (within site – 3 sec; between sites – 90mins)
    - Called SysVol (located @ system folder and is a hidden folder)
- Trust relationships supported by Win2k8
    - Transitive trust (a 2-way trust)
    - Shortcut trust (2-way)

Must be created by eadmin (root admin), the trust is 2-way, is used to speed up access to enterprise resources. Note: this is not recommended for low volume data exchange.

Nancy wants to print at a printer located in Italy. Nancy creates a token and requests from the Canada domain, Canada domain asks Namerica domain… the token continues all the way to the child domain of Italy.

- GC – ABC.com – AD – Root of forest – eadmin (enterprise administrator – SOA (start of authority))
    - Namerica
        - Canada
            - Nancy (token)
    - Europe
        - Itally
            - printer
- External trust (one-way)

External trusts are widely used with B2B related activities.

Ibm users want to print on mircosoft domain, there is a oneway trust link from the mircosoft domain to the ibm domain.

- Mircosoft.com (resources)
    - printer
- IBM.com (users/groups)
    - Users

- LDAP: Lightweight Directory Access Protocol
    - LDAP is the full path of an Object within a domain or enterprise
    - LDAP defines the following syntax(symbols)
        - CN = common name, a reference to a leaf object
            - User, group, printer, computer
        - OU = organizational unit (a container object)
        - DC = domain controller
    - LDAP path example “CN=nancy,OU=Sales,DC=ABC,DC=com”
        - Q1: what’s nancy’s LDAP path?
            - “CN=nancy,OU=sales,DC=Canada,DC=Namerica,DC=ABC,DC=com”
        - Q2: what’s laser p’s LDAP path?
            - “CN=laserp,OU=Mrkt,DC=Italy,DC=Europe,DC=ABC,DC=com”
        - Q3: Create an OU called HR below Europe domain
            - “DSadd OU “OU=HR,DC=Europe,DC=ABC,DC=com””
        - Q4: create a user called Joe below HR OU
            - “DSadd user “SN=Joe,OU=HR,DC= Europe,DC=ABC,DC=com” –

pwd passwordxxx”

Chapter 2: MB

- Windows supports both PnP and legacy hardware devices
- PnP auto detect HW devices and assign run an ID in registry
- Legacy devices need to be installed using admin password
- Windows HW provides the following installation options
    - Warn (default): sends a warning msg if the HW device is not certified

Problem: if a device is malfunctioning, you will probably get BSOD

    - Block: block all non-certified HW devices
    - Ignore: go ahead and install the device
- HW compatibility list:
    - To test your computer for certified devices
        - Sigverif.exe
- Manual HW list
    - In order to install HW Devices manually you need to know HW’s IRQ #
        - Note: IRQ (interrupt request) is a signaling mechanism used by HW devices to identify them to CPU.
    - If there is an IRQ conflict, the device won’t work
        - The following symbols are assigned
            - Red X: device is disabled
            - Yellow ?: device is detected by windows but Windows could not find a driver
            - Yellow !: driver is not compatible
    - IRQ:
        - 0: system clock: pulse generator used for CPU speed
        - 1: Keyboard
        - 2: reserved
        - 3: serial port
        - 4: serial port
        - 5: sound card
        - 6: floppy
        - 7: printer port (LPT port)
        - 13: math processor
        - 14: IDE0
        - 15: IDE1 (DVA,CD-ROM driver)
- Registry:
    - Registry is a repository area designed to hold sys info regarding installed HW and software
    - Registry is launched through:
        - Regedit command
        - Regedt32
    - Be the following main registry hives exist (5 root key):
        - HKey_local_Machine: info about all HW devices including their assigned IRQs
        - HKey_local_user: current user’s profile
        - HKey_users: default users profiles
        - HKey_Classes_Root: root definition of files and MB info
        - HKey_Current_Config:
- Virtual Memory VM:
    - Is part of HD added to the physical RAM for the purpose of OS’s operations.
        - Note: do not disable VM

- VM default size: 1.5 x physical RAM
    - Ex. If you have 2G of RAM you need at least 3G of VM

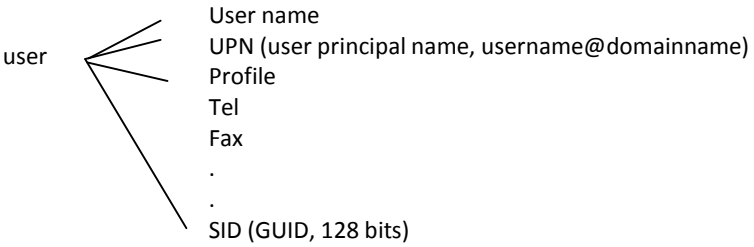
Week 4 Notes

February-01-12
10:12 AM

Domain objects (users/groups)

1 - Each domain object defined in AD, is linked to a class of Windows objects

2 - Each class (e.g. user) has at least one attribute (properties)



3 - There are 2 types of users/groups

a) Built-in:
   - Administrator
   - Eadmin
   - Backup operator
   - Server operator

   - Administrator - groups

b) User-generated accounts of groups
   1. GUI: using AD users of computers
   2. Command prompt
   3. Using Scripting languages
      - Javascript, Vbscript

GUI: The properties of a user has the following important tabs:

1. Account tab is use to manage
   - Logon hours (default 24/7)
   - Account options (password)
   - Account lockout
2. Member of (groups)
3. Profile (access to home folder, network map device)

4 - User profile

- Windows define 3 types of user profiles
  a. Local user profile: log into local computer
  b. Domain user profile (roaming profile)
     - A roaming user profile provides a set of protocols and settings such as network connection, desktop settings, shortcuts, shared folders… Provided to user as soon as he/she logs into domain
     - A roaming profile follows the user regardless of location
     - User profile is saved as a file
       - *NTuser.dat*
     - Note: Mandatory user profile is a pre-set setting that does not allow user to change the assigned profile.
       - Mandatory user profile is saved in the file (domain) called:
         - *NTuser.man*
  c. Remote desktop profile: allows users to login to domain remotely user RDP/TCP protocol
     - RDP = remote desktop protocol
     - Note: TCP provides reliable connection oriented communication

5 - User authentic an protocols:

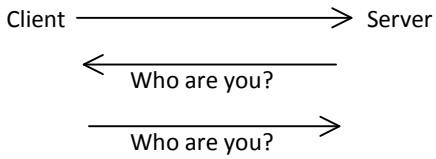
- Each user is assigned a token (token access) as soon as he/she logs successfully into domain
- The token contains the following settings
  a. Kerberos Authentication
  b. Token-Ticket: access to resources for 10 hours (default)
     - Note: User Token contains 2 components:
       a. Key distribution center (KDC)
          - Which is domain, KDC authenticates username and password combination against domain information.
       b. Ticket Granting Ticket (TGT)

- Is issued by domain to access Net Resources
- TGT is valid for 10 hours (default)
- You can change the settings by accessing Admin Tools\Domain security policy \ account policy \ Kerberos policies

6 - Authentication Protocols

- Window2k8 supports the following authentication protocols:
  a. Kerberos V5 R2
     - Domain logon authentication
  b. TLS/SSL authentication
     - SSL - HTTPS:443
     - TLS (transport layer security) - is used to access active directory objects using internet
     - *LDAP://mydomain*
  c. NTLM (NT LAN Manager) Authentication: Windows NT authentication

  Note: Kerberos authentication uses:
  - MSCHAP settings/policies
    - Microsoft Challenge Handshake Authentication Protocal
  - MS chap is a mutual authentication protocol



7 - Command prompts:

DSadd	Add a domain object
DSget	Display an object attribute
DSmod	Modify (change a domain object)
DSQuery	Query the domain
DSRM	Delete an object
DSMove	Move an object to other container (OU, Domain)

DSGet User "CN=Nancy,OU=East,OU=Sales,DC=Microsoft

Returns - Nancy's 128-bit GUID

- DSAdd user, computer, OU, group, contact
  - Important DSadd switches:
    - -pwd (Password)
    - -profile (set user's home directory, map drive)

  Example:
  DSadd user "CN=Nancy,OU=East,OU=Sales,DC=Microsoft,DC=com" -pwd Password001 -profile "\\Servername\profiles\nancy"
- DSMOD user "LDAP"
  -desc "Marketing manager"
  -fax "416-232-8932"
  -email "nancy@xyz.com"
- DSQuery List all domain users that are disabled
  DSQuery "CN=users,DC=Microsoft,DC=com" -disabled
- *DSMove user "CN=Mark,OU=Sales,DC=xyz,DC=com" -newparent "OU=Marketing,DC=xyz,DC=com"*
- *DSRM -subtree -exclude -noprompt -c "OU=Sales,DC=xyz,DC=com"*
  - About switches:
    - -subtree - a reference to OU
    - -exclude - do not delte OU itself
    - -noprompt - do not send screen msg
    - -c all objects
- DSadd user /? All command info and examples

8 - BULK import/export users

- Win2k8 objects provides powerful tools for bulk import/export domain objects. These commands are:
  a. *CSVDE -f* , object csv, object txt
     - Export all domain object to objects list

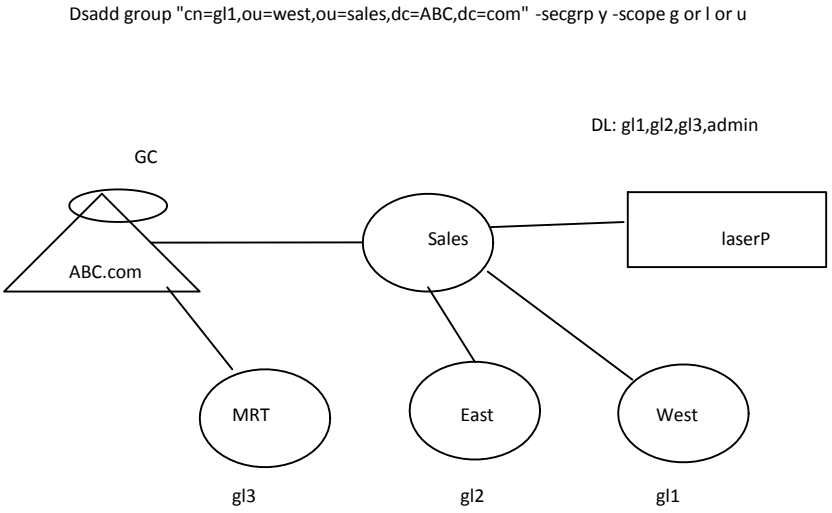
     CSVDE -i ,object txt
  b. LDIFDE , Lightweight Directory Interchange Format Directory Exchange
     - *LDIFDE -f C:\exportusers.txt -d "DC=itm315domain,DC=msft" -p subtree*

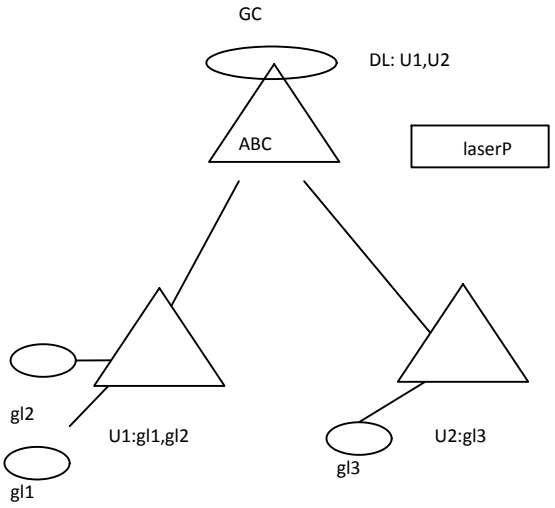
-r "(&Object…)
-l see lab 5

Week 5 Notes

February-08-12
10:16 AM

Dsadd group "cn=gl1,ou=west,ou=sales,dc=ABC,dc=com" -secgrp y -scope g or l or u

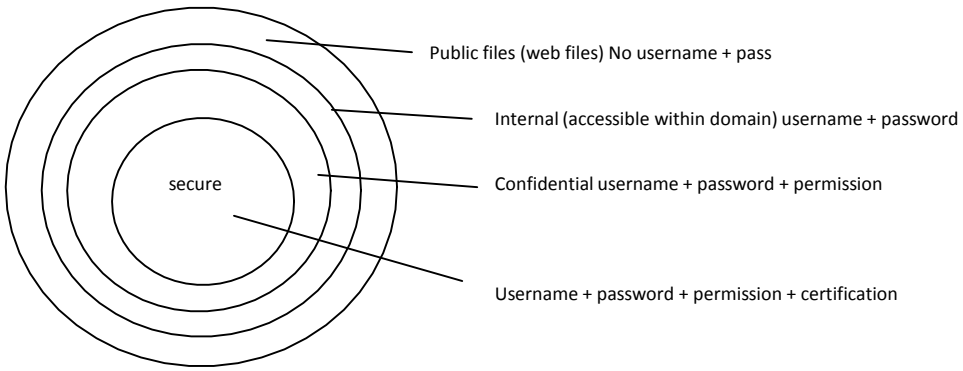




Domain Groups

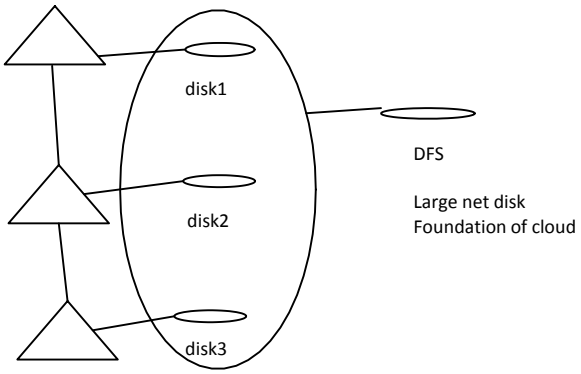
1. There are 2 types of groups
   - Security
   - Distribution
2. Security group has 3 scopes:
   - Global (default)
   - Domain local
   - Universal
3. Distribution groups
   - Are assigned to hold contacts.
   - Contacts and/or distribution groups do not have any access permissions to net resources
4. Win2k8 supports nested groups (a group within a group)
   - The global groups can be members of either l or U
   - Domain local groups may contain global or universal groups as members.
   - DL: g1,g2,g3
   - U1:g1,g2,g3
   - DL:U1,U2
5. Global groups are normally placed in Ous. Members of OU can members of global groups as well. (single domain or/and multi domain)
6. Domain local groups are created in containers that hold a net resource (ex. Printer)
7. Universal groups are created in a multiple domain structure.
   - U groups reside in Global Catalog -> faster access to enterprise resources.
8. AGUDLP strategy (enterprise)
   - Assume that an OU exists: follow the following steps:
     A. Create a user account
     G. Add user to a global group
     U. Add global groups to universal group
     DL. Add universal groups to domain local group
     P. Assign permissions to DL

File system security (chapter 5)
Layers of security

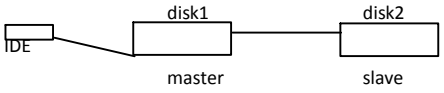


Note: Our main job is to manage confidential and secure files/folders

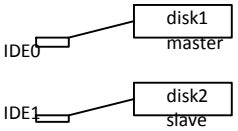
1. Win2k8 supports the following file systems:
    a. FAT12: floppy disk
        i. Max files size 1.44M
    b. FAT16: DOS File systetm
        i. Max size 2G
    c. FAT32: windows 9x file system
        i. Typical disk size 32G
    d. CD ROM file system
    e. CD DVD universal disk format (UDF)
        i. Reads writes on CD/DVD ROM
    f. NTFS (core component of win2k OS)
        i. Features
            1. Security permission on file and/or folder level
                - Ex. R means read only
            2. "unlimited" disk space
                - 16 EB
            3. Supports disk quotas
                - Limit disk space usage
            4. Supports shadow copy
                - Prevents files to be overwritten, original file will be kept when on update is triggered (ex. Excel sales file). Note: disadvantage with shadow copy a) consumes a lot disk space b) consumes net bandwidth (not files)
            5. DFS (distributed file system)
                - Global disk



6. Supports RAID system (redundant array of independent
    - RAID 0: no fault tolerant system expands physical disks up to 32 disks
        - Problem: if one disk crashes the entire drive is gone
    - RAID 1: disk mirroring/disk duplexing

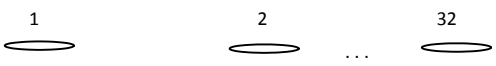


        - Disk 2 has exact identical info as disk 1 if disk 1 crashes takes over operation
        - Problem: if controller crashes no access to data solution.



More fault tolerant system

- RAID5: dynamic disk with parity is a fault tolerant system



If one disk in the chain crashes, the system receivers info on crashed disk through a mechanism called parity (logical math)

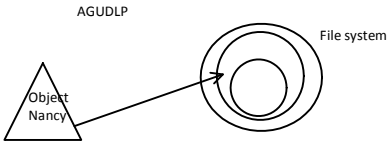
- RAID 5 supports hot swapping
    - If 2 disks crashes the entire volume gone
- Disadvantage:
    - one size of disk is used for parity info
    - Requires at least 3 disks

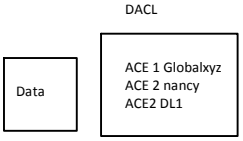
Week 6 Notes

February-15-12
10:13 AM

File Security (Part 2)
- NTFS -> RAID

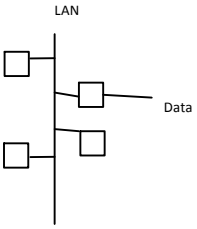
1. NTFS Features:
   a. Encryption: win2k8 EFS (encrypting file system) encryption
      - EFS uses: 56 but, 128 bit encryption (north America)
   b. Compression: Disk space
      - Note: you can not encrypt a compressed file and vice versa
      - Commands:
        - *cypher -e C:\data*.**
          - Encrypt all files located @ data folder
        - *Cypher -d C:\...*
          - Decrypt
      - Compression:
        - *Compact -c C:\data*.**
          - Compress
        - *Compact -d C:\data*
          - Decompress
   c. File permissions: win2k8 provides a feature called DACL (discretionary access control)
      - DACL is composed of entities called ACE (access control entry)





Each ACE is identified by a GUID# (128bit)

2. File Sharing:
   a. win2k8 provides file sharing and hidden files.
   - Ex.
     - C$ = hidden C:drive
     - Data$ = hidden data folder
   - Note: hidden files are accessed by the owner and admins
   b. To view shared folder:
      - *Net view* - displays all share folders except for hidden folders

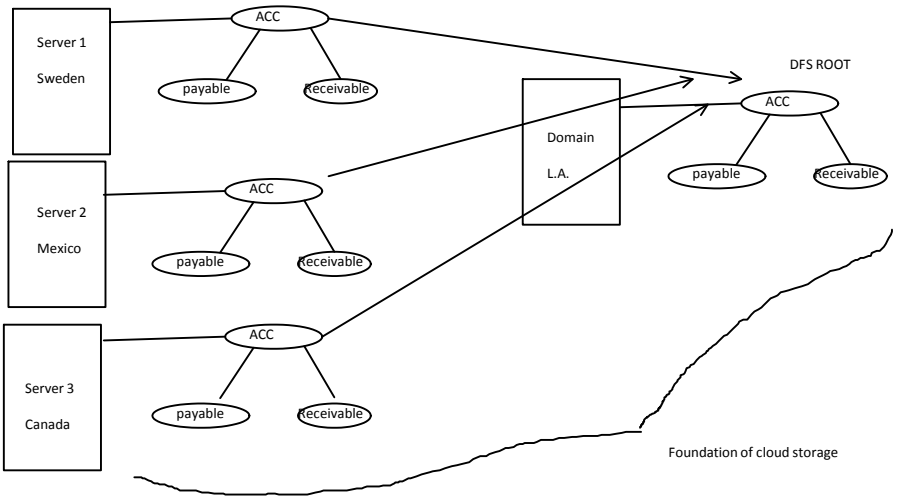


Q: Write a command that shares data folder over-the-net and hides it

Vision 1
Net Share test =C:\data
Share data folder over-the-net and name it as test folder

Version 2
Net share data$=c:\data
Share data folder and hide it

3. Distributed file system (DFS)
   - Win2k8 provides a powerful tool to create a single point of shared folder access
   - DFS is a single, logical, hierarchical file system.
   - It organizes enterprise shared folders located on globally different systems (computer) in a tree-structure format.



Advantages:
- Organize resources
- Facilitate navigation
- Facilitate administration
- Preserve
- permissions
- Provides a single point of centralized backup

Disadvantages:
- Create network traffic

   - Because the DFS tree is a single point of reference, regardless of the actual location of the underlying resources user can easily access network files:
   - DFS limitations:
     a. Max number of characters per path =260
        - Ex. \\server1\acc\payable (26 chars)
     b. Max number of volumes (H.D) 32
     c. Max number of DFS root: server = 1
     d. Max number of DFS root: domain = unlimited
   - Types of DFS
     a. Stand-alone DFS
        - Permits a single level of DFS links
        - Exist on a local computer (server)
        - Offers no replication or centralized backup
        - Provides one root DFS
     b. Domain:
        - AD integrated file system
        - Provides replication
        - DFS is part of GC
        - Supports centralized backup
        - Supports unlimited DFS roots

Attribute command:
- The following file attributes exist:
  - R = read only
  - S = system
  - H = hidden
  - A = archive
- Boot.ini
- Attrib -s-r-h C:\boot.ini
  - Remove system , hidden of read only attribute
- Attrib +s+r+h C:\boot.ini
  - Q: drive F: is a FAT32 file system convert it to NTFS
  - Convert f: /fs:NTFS

  - Q: the following folder structure exist in C:
    - C:\\data\weekly\project each folder contains files

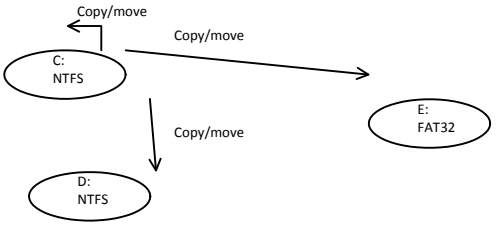
Copy/move

- Q: drive F: is a FAT32 file system convert it to NTFS
- Convert f: /fs:NTFS

- Q: the following folder structure exist in C:
  - C:\\data\weekly\project each folder contains files

  Write a command that copies the entire data folder to f: including empty folders

  A: *xcopy C:\data*.* f:\data /s /e /y*



1. What happens when you copy data folder located in C: drive to another location under C:?
   - It retains its original permissions
2. Copy C:\data to D: permissions?
   - Inherits permission from destination
3. Copy C:\data to E: fat32 permissions?
   - FAT32 does not support file security
   - All users have full control on data flow
   - Data folder loses its security

- Move operation:
  1. Move data folder from C: NTFS partition to another location within C: drive permissions?
     - It retains its original permissions
  2. Move C:\data to D:NTFS permissions?
     - Inherits permissions from destination
  3. Move C:\data to FAT32
     - Data folder loses its original permissions
     - All users have full control on data folder

Midterm Review

February-15-12
11:55 AM

Time: 1.5 hours
Starts @ 10 am
Format: around 40 MC (40marks)
Written part 4 to 5 short answers (25-30 marks)

Main topics

Understanding domain infrastructure

- Trust relationships
- Replication: within sites and between sites
- Multi master vs. master/slave
- Define site
- Define AD
- Define GC

Object exist in GC are:

a. Enterprise objects + universal groups
b. Domain commands:
    1. Objects creation: Dsadd "LDAP"
    2. Create domain groups: Dsadd group "LDAP"
    3. Combination: ex. Dsadd "CN=nancy,OU=west,ou=sales,dc=abc,dc=com" -password pass01 -memberof "LDAP of group"
    4. SID
    5. Modify -desc -fax -email
    6. Create group -secgrp y -scope l
c. Understand the role of domain groups
    - Types
        1. Security
        2. Distribution (contacts)
    - Scope
        1. Global
        2. Local
        3. Universal
    - AGUDLP strategy
d. misc.

File system

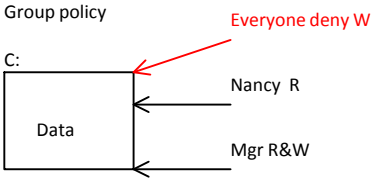
- Types of file system
- DFS
- NTFS features
- RAID
    - RAID0 (disk dynamic)
    - RAID1 (fault)
    - RAID5 (fault)
- Move and copy operations
- Today lec.
- File system commands
- Misc.

Final exam is 50/50

Week 8 Notes

March-07-12
10:14 AM

File Management
Group policy



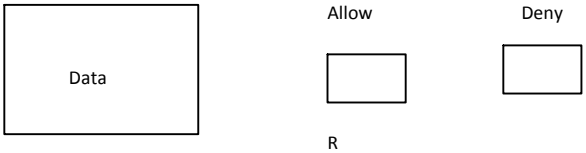
Note: nancy is a member of mgr
Q1: what is nancy`s effective permission on data folder?

1. Effective permission
   Cumulative = user permission + group permission (if any)
   Effective permission = R + R&W = R&W

Q2: Nancy is a member of group everyone. This group is denied W permission. What is nancy's effective permission?

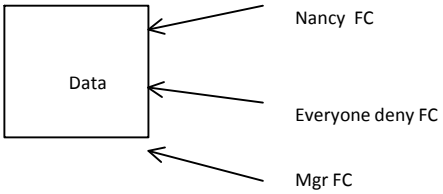
2. Permission over-the-net
3. Deny or Allow
   Deny always overrides allow permission.
   Deny full control = no access

1) Security Permissions



R
R&W
C = Create
D = delete
M = modify
FC = Full Control

R = Read content + execute app (if any)
W = open an existing file and change the content
C = create a new file/folder
D = a permission to delete files/folders
M = all of the above + change file/folder attributes
FC = M + take file/folder Ownership
(be very careful assigning FC to users)



Nancy & joe are members of mgr group
Nancy is also a member of everyone

Q3:
QA: nancy's effective permission on data folder
No access deny takes over

QB: Joe's effective permission on data folder
FC

Q4: If everyone was deny modify. What is nancy's effective permissions?
FC - M = take ownership permission

2) Shared Folder permissions

Shared folder security contains 2 parts
a. Local security permissions
b. Over the network permissions

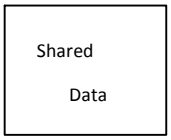
Over the network permissions:

The following permissions are assigned to a shared foler:

- Read
- Change (change is always = to modify on NTFS)
- Full Control

Data Folder Example:

Data folder is shared over the network. With the following security settings (permissions).



Permissions

User Group	NTFS	Shared
Nancy	M	R
Mgr	C	FC

NTFS = logon locally (in this context)

Q1: What is nancy's effective permission when she logs on locally?

M (which contains C)

Q2: What is nancy's effective permissions when she accesses the folder over the net?

Nancy	M	R
Mgr	C	FC
Cumulative	M	FC

Most restrictive --> M

Note:

1. Over the net permissions contains NTFS permissions and shared permissions.
2. If there is a conflict between shared and NTFS permission the most restrictive permission is applied (from shared or NTFS)
3. If there is a conflict between allow permissions and deny permissions deny is applied
4. By default group everyone has R permissions on NTFS and shared folders.

Example 2:

Data folder is shared over the net

Users/groups	NTFS	Shared
Joe	R&W	Change
Nelly	FC	Read
Mgr (J,Ne)	M	Change
GroupG (J,Ne,Na)	R-W-C	Read Deny

Q1: what's joe's effective permissions when he logs locally?

R&W + M + R-W-C = M

Q2: What's nancy's effect permission over the net

NTFS = R-W-C

Shared = deny read

Permission: W&C + Deny Read

Q3: What is nelly's effective permission when she logs locally?

FC + M + R-W-C = FC

Q4: What is nelly's effective permission when she accesses the folder over the net?

NTFS = FC

Shared = R + Change + Deny Read = Change & Deny Read

Permission: Change & Deny Read

Example 3

User	NTFS	Shared
Alex	FC	Deny FC
Bell	RWCD	Deny Change

Q1: What's alex effective permission over the net?

No Access

Q2: Bell over the net?

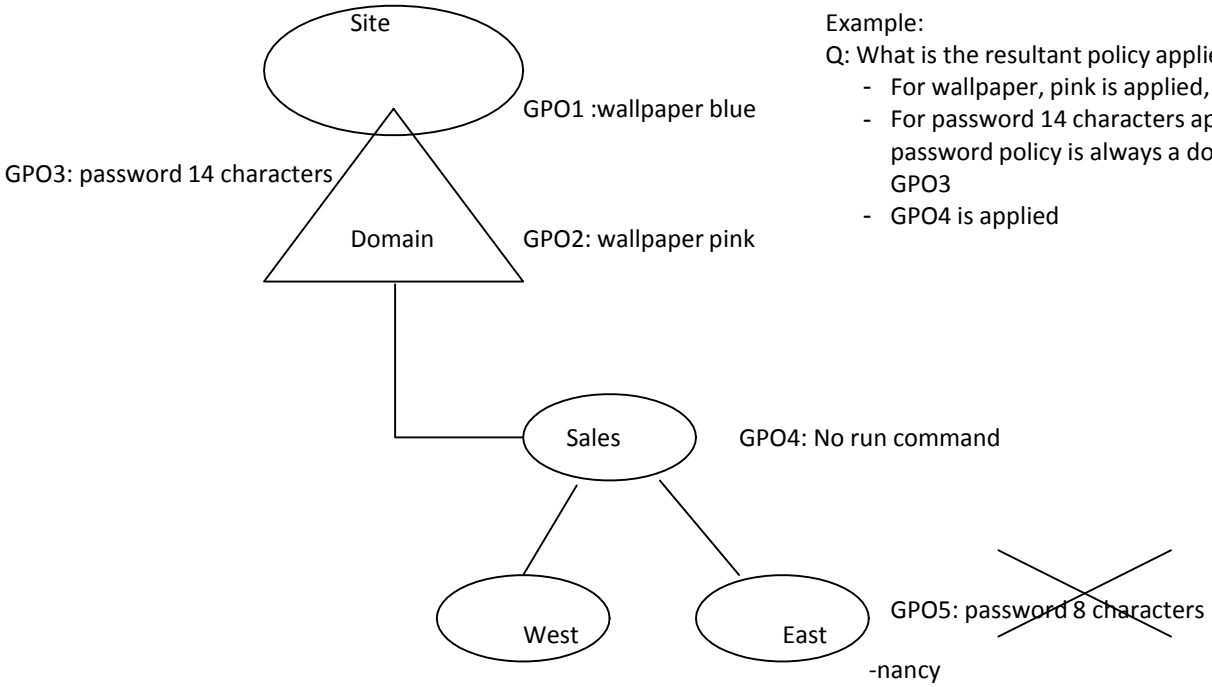
Deny Change

Week 9 Notes

March-14-12
10:32 AM

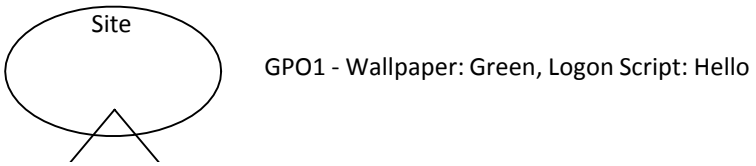
Group Policy Object (GPO)

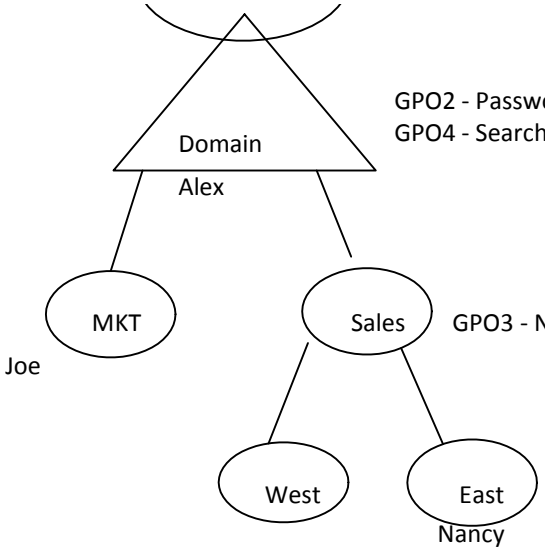
1. Definition: A GPO is an object that is used to
    - Control users desktop and network environment
    - Control network security (IPsec)
    - Apply login scripts
    - Deploy software
2. A GPO contains
    - GPT
        - Group Policy Template - Contains the actual group policy settings (data).
        - GPT is located at %systemroot%\Sysvol
        - Note: Sysvol is a folder that contains: GPT, Active directory replication data, scripts (logon\logoff), and more
    - GPC
        - Group Policy Container - located in Active Directory
        - Identified by its GUID
        - Contains Version #
3. Group Policy Conflict Resolution
    - The order of GPO
        - Local computer, site, domain, parentOU, child OU.
            - □ If there is no conflict between policies, all policies are applied.
            - □ Security policies such as
                - ◆ Password policy
                - ◆ IPsec policy
                - ◆ Account lockout policy
                - ◇ Are <u>domain policies</u> only
            - □ For non-security policies, the policy applied last (child OU) is applied.



Example:
Q: What is the resultant policy applied to nancy?

- For wallpaper, pink is applied, GPO2
- For password 14 characters applied because password policy is always a domain level policy, GPO3
- GPO4 is applied





GPO2 - Password: 8 char, logoff script: bye, no run command
GPO4 - Search Command Enabled, No computer icon on Desktop

GPO3 - No Search Command, No CD-ROM Drive, Run Command Enabled

GPO5 - MS Office Package, Logon script: Hello Welcome,
Logoff script: Please do not leave lights on

Example 2:
Q:1 What is Alex's resultant policy?

- GPO1
- GPO2
- GPO4

Q2: What is Nancy's resultant policy?

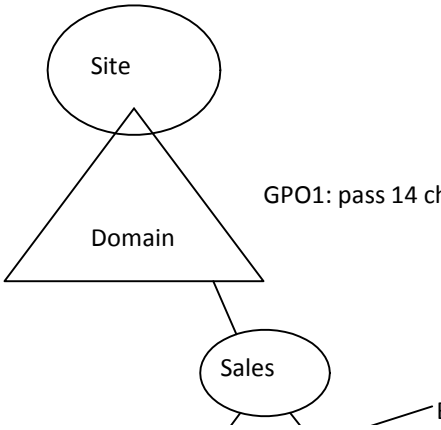
- Wallpaper: Green, GPO1
- Logon script: Hello Welcome, GPO5
- Logoff script: Please do not leave lights on, GPO5
- Run Command Enabled, GPO3
- No Search Command, GPO3
- NO CD-ROM Drive, GPO3
- NO desktop icons, GPO4
- MS office applied, GPO5

Q3: What is Joe's resultant policy?

- GPO1
- GPO2
- GPO4

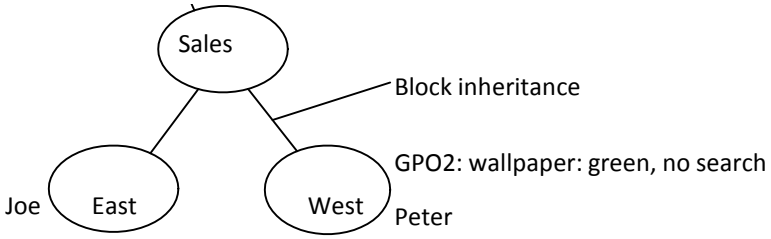
4. GPO Modes
   - There are 2 deployment modes
     - No override (enforce policy) - parent level
     - Block inheritance
   - When "no override" option is selected the GPO is forcibly applied on all child-containers
   - When "block inheritance" is selected, the non-security policies are blocked.
     - In other words we cannot block security policies at child level, however non-security policies can be blocked
   - Note: by default, non of the above options are activated

Example 3



GPO1: pass 14 chars, no run command

Block inheritance

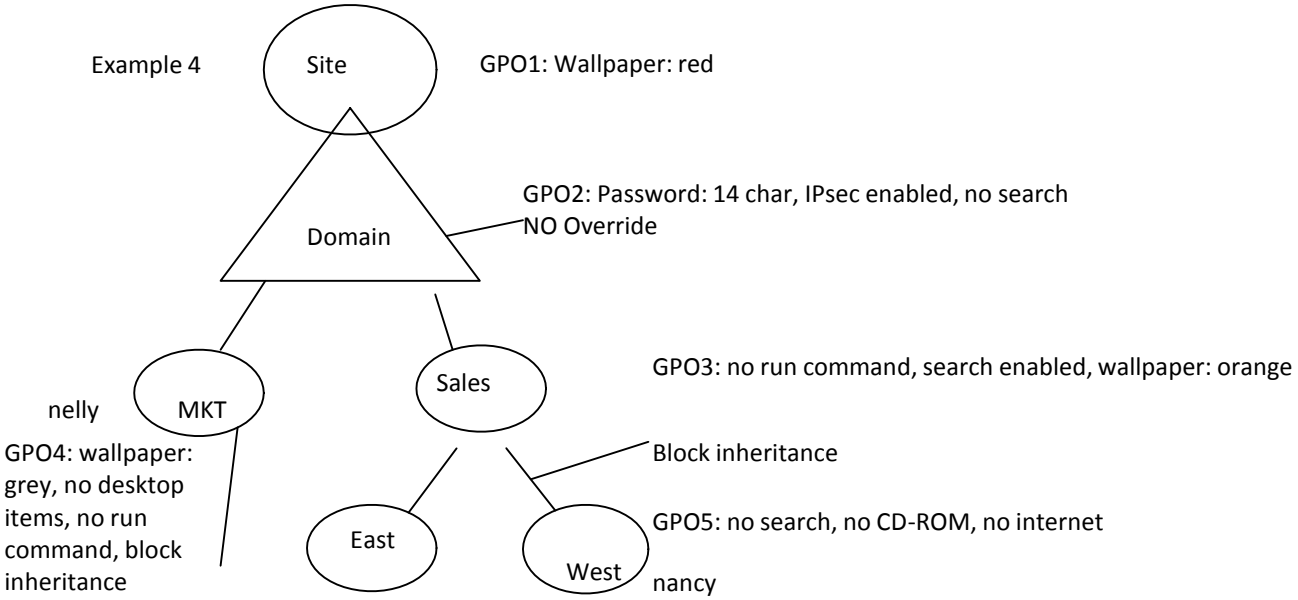


Q1: What is peter's resultant policy?

- Password: 14 chars, wallpaper: green, no search, run command remains enabled

Q2: What is Joe's resultant policy?

- GPO1



Q1: nancy's resultant policy?

- Password 14 char, IPsec enabled, GPO2
- No search, no CD-ROM, no internet, GPO5
- Run command enabled
- Wallpaper: default

Q2: nelly's resultant policy?

- GPO2 + GPO4

Week 10 Notes

March-21-12
10:09 AM

Group Policy Part 2:

- GPO (group policy object)
  - GPT (group policy template)
    - Located in sysvol
  - GPC (group policy container)

1. Managing Security using GPO

- Security policy is applied at domain level only
- Domain security settings contain the following main nodes:
  a. Account policy
     i. Password policy
     ii. Account lockout policy
     iii. Kerbros policy (token - based policy)
        - Note: kerbros policy is referred to as Ticket Granting Ticket (TGT) policy. TGT is used to modify user Token setting such as the ticket life time (token).
  b. Local policy
  c. Public key policy (PKI) public key infrastructure
     i. PKI
        1) Public
           - Plain text + public key -> encrypted message (the public key belongs to the receiver)
        2) Private
           - Encrypted message + private key = plain text (the private key belongs to the receiver)
  d. Software restriction policy (firewall)
  e. IPsec policy
     i. Server (request IPsec)
     ii. Client (Response)
     iii. Secure server (enforce IPsec)

2. Managing users desktop environment using administrative template

- Administrative templates are register based settings
- Administrative templates can be applied on users and computers
- If there is a conflict between computer GPO settings and user configuration **the computer policy** is applied.
- There three main categories of settings:
  a. Locking down the desktop
     - Hide all icons on desktop
     - Don't save settings at exit
     - Hide specified drives in my computer
     - Disable and remove links to windows update
  b. Locking down users access to net resources
     - Hide my network places
     - Disable internet option
     - Remove "map network drive"
  c. Locking down users access to administrative tools and applications
     - Disable changes to taskbar and start menu
     - Remove search menu
     - Remove run command
     - Disable task manager
     - Hide program groups in start menu

3. Software settings (publish/deploy software)

- Used to install software packages (.msi - microsoft installer) over the network
- Used to remove or upgrade application software. There are three options:
    - Force (enforce remove/upgrade)
    - Optional
    - Not defined (default)
- Publish: A publish software package is not advertised in start menu, it is placed in add/remove programs in control panel.
    - Applications can publish to users and NOT computers
- Deploy: a deployed software package can be applied on users or computers.
    - The deployed software will be appeared in start menu.
    - The deployed software is activated (triggered) for installation through:
        a. User action (double clicking)
        b. Using start menu for installation

4. Windows settings:

- Provides:
    a. Script: you can use VBScript or JavaScript to send msg to users during:
        - Computer config
            - Computer startup
            - Computer shutdown
        - User config
            - User logon
            - User log off

        If both applied: start up, logon, log off, shut down
    b. Folder redirection
        - Advantage:
            1. Data is always available to users
            2. Data is centrally stored for backup
            3. Files are not saved on client PCs or working stations
        - Disadvantage:
            1. Generates network traffic
        - The following folders can be redirected
            1. My document
            2. Desktop
            3. Start menu
            4. Application data (ex. Database)
    c. Internet settings
        - How the user interacts with the internet and its applications

5. Security Templates:

- Are pre-defined configurations that an administrator can use to deploy microsoft standard config
- Security templates have extension: .inf
- The following main security templates exist:
    - Security .inf (default server security setting)
    - DC security .inf (default domain security setting)
    - SecureDC .inf (a higher level domain security)
        - Ex. Is not backward compatible with win2k3
    - HiSecDC .inf (The highest level of domain security)
- You can apply security policy on WSs.
    - SecureWS.inf
    - HiSecureWS.inf (highest security)

- GPResult.exe /s domain computer name /u
    - Returns the group policy resultant for specified user
- DCpromo.exe

    - Installs domain
    - Note: DCpromo.exe is used to promote a server to a domain:
        - The same command is used to uninstall the domain. You have to be root administrator (eadmin)
- Example:
    - GPResult.exe /s itm315 /u itm315domain\nancy
        - Returns the resultant policy(ies) applied to nancy

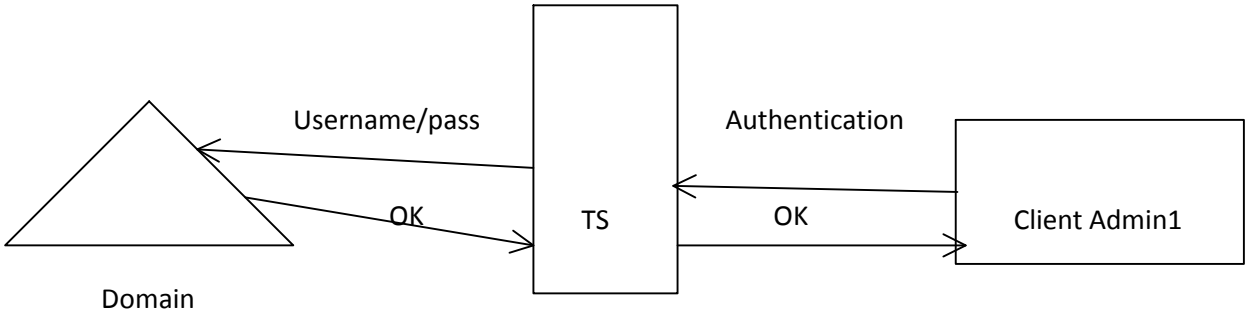
Week 11 Notes

April-04-12
10:10 AM

Server Administration

- MMC files have extension .msc (management saved console)
- MMCs are used to admin Domain environment
- A Simplified MMC is called taskpad
- Taskpad contains shortcuts to domain tools
- Taskpads are created by Domain Admin and distributed among some users to help Admin's daily work.

Terminal Services



- TS servers are integrated in AD
- Terminal Serer uses a protocol called RDP/TCP protocol

Note: UDP - Broadcast, faster, does not guarantee msg deliver; TCP connection-oriented protocol, guarantees msg delivery (error-handling), slower than UDP.

- RDP uses port# number 3389
- RDP was introduced in windows to provide remote access to server.
- All MS client machines are shipped with remote desktop program.
- By default win2k8 server provides one permanent EDP license
- By default EDP is installed on win2k8 server but disabled. To enable: right-click my computer> properties>remote desktop
- Using administrative password you are able to modify/setup client's remote desktop connectivity.
- You are able:
    1. Configure TS profile: A profile used by remote users
    2. Remote control: settings for remote connectivity control and network environment.
        i. Ex. Hide IP
    3. Session: to control idle times (ex. 20mins)
    4. Environment: is used for remote scripts.

SUS - Software update services

Clients --> SUS <-- Mircosoft.com

- This service is enabled by default (client and server)
- Properties of my computer>automatic update>check keep my computer up to date.
- Three windows update options:
    1. Notify me before downloading
    2. Download the updates automatically & notify me when they are ready to install
    3. Automatically download and install them on schedule time.

- SUS replaces the above windows options using its own admin defined settings.
- SUS is used to update windows only
- SUS can not be used to update 3rd party software packages
- SUS can be managed through the internet, http://serverIP/susadmin
- You can remotely access the following options:
    - Monitor server
    - View log files
    - Approve windows update
    - Synchronize the server
- To enable SUS for clients; you need to publish/deploy SUS client software. SUS client package is called: WUAU22.msi
- Disadvantage
    - SUS needs huge storage
    - SUS generates a lot network traffic => update clients off office time.

Cloud computing and server vitualization

- A cloud system is used to provide three services to potential clients (e.g., companies, universities, government, individuals)
- Services:
    - Saas
    - PaaS
    - Iaas

- These services are provided on-demand. On-demand -> client are chanrged based on # of hours they used the cloud system.

- Grid computing
    - Grid computing is a service provided to clients who had computing resources demand. Ex. Media application, research application.
    - Grid providers are company that provide supercomputer resources to application intensive clients.
- Note: There 2 ways to increase computing power:
    a. Having high-end sys (mainframe, supercomputing)
    b. Using distrbuted systems

Hyper-V server:

- Hyper-V is used as a means of implementing server virtualization.
- You can have up to 64 servers installed into a single machine.
- Hyper-v provides also platform for multiple.
- Hyper-v provides also platform for multiple OSs
- Hyper-v provides up-to 256 virtual desktops
    - => greenIS (greenIT)

Hyper-v -- azure (db) } cloud

Advantage:

- On demand
- Available 24/7
- Can be delivered to any IP enabled device (VD)
- High speed

Disadvantage:

- Security
- Fault tolerance
- Cost (for enterprise companies a cost saving approach)

Disaster Recovery

- Backup
    a. normal, full backup (backs up everything) and removed 'A' worker.
    b. Incremental: it backs up everything since the last full backup, and removes the marker.
    c. Differential backup: backup all files folders create/uploaded since the last full or incremental backup, it does NOT remove the marker.
        i. Tuesday diff backup contain mondays diff backup files.

  Note: normal, diff and incremental backups can be scheduled using windows backup.

    d. System files backup
        i. OS core files (system files)
        ii. Sysvol
        iii. AD
        iv. Security files
    e. Copy.

  Scenario 1: Faster backup, slower restore
  Your company's backup policy is as follow:

- Sunday: full backup
- Mon-sat: incr. backup

  On Friday @ 11am server crashed. How many tapes do you need to recover from crash?
  1 tape: full backup
  Mon-Thursday: 4 tapes

  Scenario 2: slower backup, faster restore
  Sunday: full backup
  Mon-sat: diff backup
  Friday @ 11am crash.
  1 tape Sunday (full backup)
  1 tape Thursday (Thursday contains Wednesday backup)

  Scenario 3:
  Sunday: full backup
  Mon-weds: incr. backup
  Thursday-sat: diff backup
  On Saturday 10am server crashes
  1 tape of Sunday
  3 tapes mon-weds
  1 Friday

Grand Father - Father - Son

  Tape = rotation scheme:
  Son: daily backup (rotate)
  Father: weekly full backup (rotate)
  Grandfather: month full backup (keep)
  --> @ the end we have 12 tapes (jan, feb, mar) one-onsite, one off site.

Final Exam Review

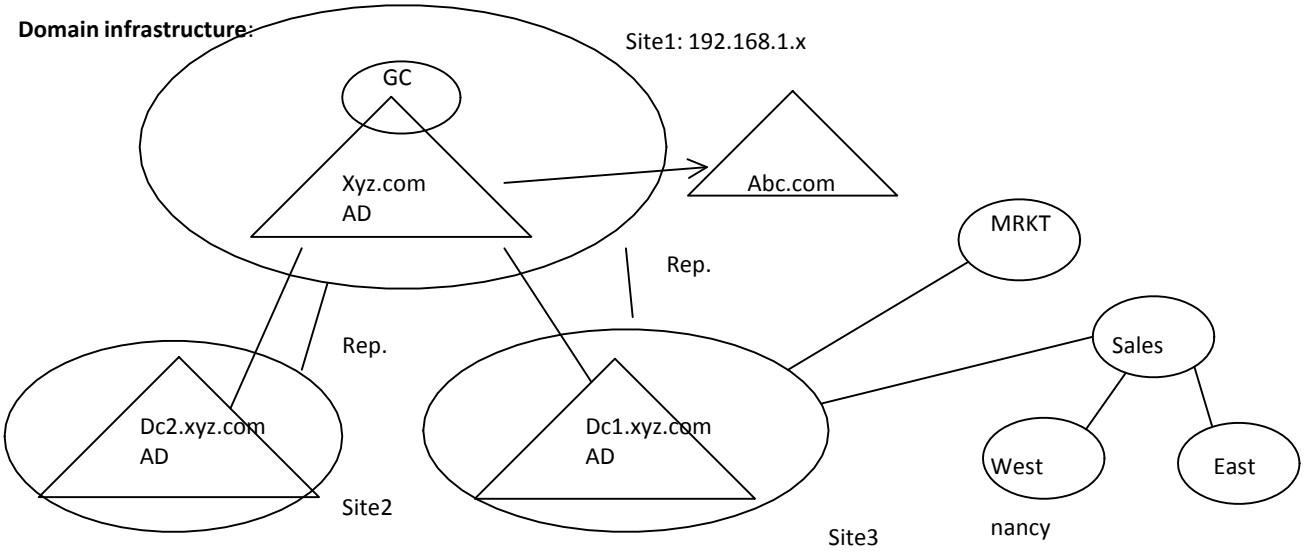
April-11-12
10:09 AM

- 2 hours
- Part 1: MC (50%)
- Part 2: Short Answer (50%)

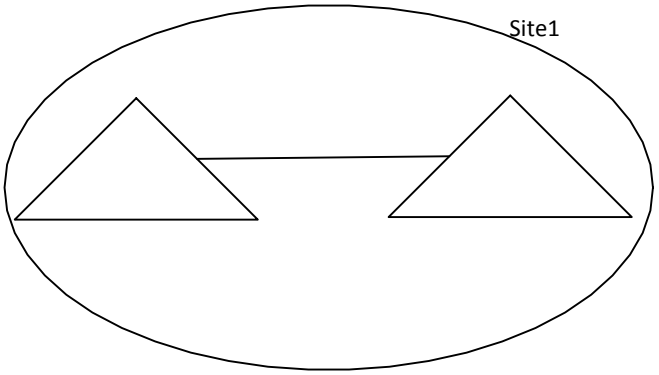
5 Main Areas:

1. Domain infrastructure
2. User objects (Domain Objects)
3. Files System
4. Group Policy Object
5. Server Admin/Server Hardware

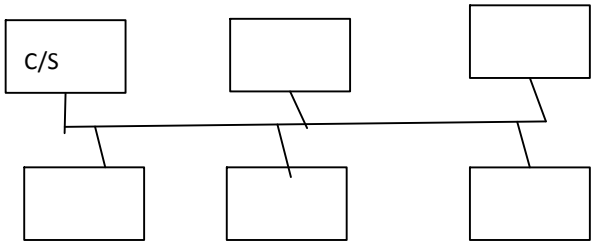
Domain infrastructure:



- Trust Relationships
- Transitive trust (2-way)
- Shortcut (2-way)
- One-way external
    a. Trusting
    b. Trusted
- AD: a DB of domain objects
- GC: Root Domain
- Site: Defined by IP
- Replication
    - Within sites
    - Between sites
    - Urgent (security)



- Rep time
    - 2 types if networks:
        - P2P Network
        - Client/Server



No Dedicated Server (very active client/very passive server)

Max supported WS: 10

Win 2k8 server supports unlimited clients

Domain Objects:

- AD is a Database arranged based on LDAP protocol
  - Any query against AD should follow LDAP rules
- LDAP is IEEE/IETF protocol (internet eng. Task force)
- Using LDAP win2k8 OS can talk to Linux, UNIX
- LDAP is used to locate an object within an enterprise domain
- Win2k8 provides the following commands to create/locate/update an object
  - DSADD user, group, computer, contact, OU "LDAP path"
- DSget SID=128 GUID
- DSMod
- DSRM -c -exclude
- DSMove -subtree

- Groups
  - Built-in groups (administrators, everyone)
  - User generated groups
  - GROUP
    - Type
      - Sec
      - Dist -> members called: contact (email)
    - Scope
      - Global
      - Local
      - Universal
  - Create a domain local group in sales called DLS
    DSAdd group "CN=DLS,ou=sales,dc=dc2,dc=xyz,dc=com" -scope l -secgrp yes
  - a. Dsadd a user and make that user a member of DLS group
  - b. Dsadd a group and make that group a member of DLS
  - User profile
    - Domain profile (roaming profile)
      - Roaming
      - Mandatory roaming
    - Local user profile
    - Remote desktop profile
      - Terminal services
  - Bulk import/export user
    - -f export(out)
    - -i input

File System:

- Types of file systems by w2k8
  - Fat12: 1.44 M (FD) IRQ 6
  - VFAT
    - Fat16: 2G
    - Fat32: 32G
  - NTFS: 16EB
- NTFS:
  - RAID:
    - RAID0 (dynamic disk, no fault tolerant, up to 32 HD)
    - RAID1 (mirroring, duplexing)
    - RAID5 (striped disk with parity, best fault tolerant, 3-32 disk, one disk for parity)
- DFS
  - Standalone DFS
    - 1 root, no backup support, replication
  - Domain based
    - Unlimited root, backup and replication support
- Shadow copy

- Security
  - File system security
    - Copy and move
- Sharing
  - Sharing command
    - Netshare data=c:\data
    - Data: shared named, C:\data: physical location
    - Hidden shared data$ (Hidden data)

    Note: you can share any folder located @ NTFS or FAT system including CD/DVDs
    NTFS: high security
    FAT: no security
- NTFS
  - R, W, C, D, M, Full Control
- Sharing
  - R, Change, Full control

a. local acc
b. over-the-net

Server Virtualization

- Hyper-V
  - Green IT (IS) project
  - Cloud Computing
    - SaaS
    - PaaS
      - Server virtualization
      - Support for multiple platform
      - Virtual desktop
    - IaaS
  - TS
  - SUS